UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,971	02/27/2002	Gregory Eugene Perkins	10013820-1	1209

7590 12/28/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
CHANKONG, DOHM	
ART UNIT	**PAPER NUMBER**
2152	

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/085,971	PERKINS ET AL.	
	Examiner	Art Unit	
	Dohm Chankong	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1> This action is in response to Applicant's amendment and request for continued examination. Claims 1-59 are presented for further examination.

2> This is a non-final rejection.

Continued Examination Under 37 CFR 1.114

3> A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10.20.2005 has been entered.

Response to Arguments

4> Applicant's arguments with respect to claims 1-5 and 21-30, rejected under 35 U.S.C § 102(e) have been considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

5> Applicant's arguments filed 10.20.2005 in regards to the 35 U.S.C § 103(a) rejections have been fully considered but they are not persuasive. Applicant has amended claim 6 (and other independent claims) to more particularly define the various network devices within the system and argues in substance that the combined references of Win and Brown are deficient

in regards to functionality of "application server (operating on a first network device) that provides a data service (operating on a second network device) with the temporary credentials to access and interact with the data service on behalf of a client device. Those temporary credentials are generated by the data service according to a profile located by an identification service that operates on a third network device. The identification service locates the profile using profile data provided by the client device" [See Applicant's arguments, pages 19-20].

6> Win is directed towards a role-based system for securely allowing certain users access to protected resources [abstract]. To achieve this system, Win discloses several components working collectively: the user system, access server, registry server and a protected server [abstract]. In the context of Win's system, his access server executes a run-time module which corresponds Applicant's claimed first network device and application server, respectively. His protected server, with protected resources corresponds to Applicant's claimed second network device and data service respectively. Win's registry server corresponds to Applicant's claimed identification service. Win discloses a clear delineation of responsibilities for each of his devices that substantially correspond with Applicant's claims. For instance, a user first logs in through an access server. Before the user can access a protected resource located in the protected server, the user's profile must first be accessed at the registry server, which is returned as a cookie such that the user may access the protected resource [column 6 «lines 20-57»].

As discussed in the previous action, Win did not expressly disclose that his

access server and run-time module obtained the cookie (temporary credentials) to access and interact with the protected resource on behalf of the client. Rather, Win teaches a conventional method where the cookie is returned directly to the user browser.

Brown was utilized as a teaching that improved upon this method for providing cookies in a system. Brown discloses that the cookie is returned to a network device, whereby the network device utilizes the cookie to access and interact with a desires resource on behalf of a client [0012]. Brown discusses that the benefit of such a feature provides increased security and ease of use for the end-device because the proxy handles all cookie-related processing [0026, 0027]. Thus, Brown modifies Win's system such that Win's access server acts with the same functionality taught in Brown's proxy server. The cookie that is returned by Win's registry server is now directed and processed by the access server who accesses and interacts with the protected server on behalf of the user.

Based on the preceding remarks, Applicant's arguments are not persuasive, and the claim rejections under 35 U.S.C § 103(a) are maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7> Claims 1-5, 21-25, and 26-30 are rejected under 35 U.S.C § 103(a) as being unpatentable over Win et al, U.S Patent No. 6.453.353 ["Win"], in view of Brown et al, U.S Patent Publication No. 2003|0061275 ["Brown"].

8> Win was cited by Examiner in previous Office Action, dated 4.15.2005.

9> As to claim 1, Win discloses a method for providing a first network resource operating on a first network device access to a second network resource operating on a second network device, comprising:

from a third network device, locating a profile using profile data obtained from a client device, the profile containing data for identifying and for accessing the second network resource [Figure 4 «items 106, 208, 108» | column 5 «lines 44-54» | column 7 «lines 45-57» | column 10 «lines 45-55» where : Win's access server contains a protected resource, uses user's identification to request the user's profile from a registry server (which corresponds to the third network device), the user profile containing the user's roles, the roles defining resources accessible to the user];

from the third network device, supplying the profile to the second network resource [column 10 «lines 45-49» where : Win's registry server corresponds to the third network device]; and

from the third network device, receiving, from the second network resource, temporary credentials for accessing the second network resource and generated according to the profile [column 6 «lines 48-54» | column 10 «line 51» to column 11 «line 9» where : Win's

access server generates a temporary cookie that is transmitted to the user, and the cookie provides the information that enables a user to access his resources based on his profile (role)].

Win discloses that the temporary credentials are provided to the client and does not expressly disclose providing the first network resource (here Win's access server) with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access the second network resource on behalf of the client device.

10> As discussed in the response to arguments, Brown discloses providing the first network resource with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access the second network resource on behalf of the client device [0012, 0026, 0027 where : the proxy server is supplied with the temporary credentials from the web server]. Thus, it would have been obvious to modify Win's access server with the functionality taught by Brown's proxy server. Providing such a combination enhances the security of the system [see Brown, 0011].

11> As to claim 2, Win discloses the method further comprising the act of invalidating the temporary credentials following a termination event [column 11 «lines 6-9» where : a cookie can be set to expire].

12> As to claim 3, Win discloses the method wherein the termination event involves the lapse of a set time period [column 11 «lines 6-9»].

13> As to claim 4, Win discloses the method wherein the termination even involves the first network resource accessing the second network resource [column 11 «lines 6-7» where : when a cookie expiration is set to 0, the cookie is not saved on a computer. That is, a cookie is used once for a session and then the cookie expires].

14> As to claim 5, Win discloses the method wherein the temporary credentials that provide limited access to the network resource [column 11 «lines 53-64» where : the personalized menu contains only those resources that are accessible to the user]. Win does not expressly disclose that the first network resource accesses the second network resource. However, see rejection of claim 1 for combination of Win-Brown.

15> As to claim 6, Win discloses a method for enabling an application server to access a data server, the application server operating on a first network device and the data service operating on a second network device [Figure 1 «items 106, 112»] comprising:

the application server instructing a client device to provide profile data to and identification service operating on a third network device [Figure 1 «item 108»], the identification service having access to one or more profiles used to access one or more data services including the data service operating on the second network device, the profile data identifying a particular profile [Figure 1 | Figure 4 «items 106, 410, 108» | column 5 «lines 44-

54» | column 9 «lines 33-60» | column 10 «lines 45-55 where : Win's access server corresponds to an application server requesting a profile from Win's registry server];

the identification service locating the particular profile using the profile data received from the client device, the profile containing data for identifying and for accessing the data service [column 10 «lines 45-55»];

the identification service providing the profile to the data service [Figure 4 | column 10 «lines 47-49» where : Win's HTTP server, runtime module, and protected resources are provided with the profile from the registry]; and

the data service generating temporary credentials for accessing the data service identified by the particular profile [column 6 «lines 48-54» | column 10 «lines 55-63» where : the HTTP server generates a cookie for the user to access the protected resources, the HTTP and resources part of the access server data service].

Win does not expressly disclose that the application server obtains the temporary credentials and providing the data service with the temporary credentials to access the data service on behalf of the client.

16› In a related field of invention, Brown is directed towards a system for enabling a user to access resources. Brown further discloses a system that enables a proxy device to access the resources using credentials and rights of a user device Brown discloses an proxy server obtaining temporary credentials that were generated for a client, and provides a data service with the temporary credentials to access the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the

temporary credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple locations[0026, 0027]. Brown's system is analogous with respect to Win except Brown's proxy server provides the added functionality of being able to act for the client by providing the necessary credentials (in this comparison, Win's access server would correspond to a proxy). Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

17› As to claim 7, Win discloses the method wherein the act of instructing the client device includes providing a user interface that includes instructions to send profile data to the identification service, and sending the interface to the client device [Figure 5A «item 504»].

18› As to claim 8, Win discloses the method wherein the act of instructing the client device comprises redirecting the client device to the identification service [Figure 4 «items 402, 406, 414» | column 9 «lines 23-27»].

19› As to claims 9 and 10, as they do not teach or further define over the claimed limitations of claims 2 and 5, respectively, they are rejected for the same reasons set forth for claims 2 and 5, supra.

20› As to claim 11, Win discloses the method further comprising the application server generating an interface includes generating a framed web page having a first frame and a second frame, the method further comprising providing, for the first frame, content for directing an application, and providing, for the second frame, content for selecting one or more electronic files managed by the data service identified by the specified profile [column 5 «lines 44-46» | column 6 «lines 10-16» | column 9 «lines 20-30» | column 11 «lines 33-64» | column 12 «lines 3-8 and 65-66» where : Win's roles are analogous to user profiles. And Win discloses web pages with functionality for directing an application and selecting one or more electronic files but does not explicitly disclose that the two functionalities are split amongst two frames but does disclose that the user options are presented in a personalized HTML menu and that the browser should be compatible with frames. Frames are ubiquitous in the art and therefore would be expected in Win's HTML pages. The claimed use of a first frame and second frame is merely a design choice and does not represent any patentable distinction over the prior art references].

21› As to claim 12, Win discloses the act of sending the profile data includes sending a cookie identifying the particular profile upon opening the framed web page. [column 8 «lines 23-31» | column 10 «lines 51-54» | column 12 «line 65-66» | column 19 «lines 3-5»].

22> As to claim 14, Win discloses a method for enabling an application to access a data service, the application server operating on a first network device and the data service operating on a second network device [Figure 1 «items 106, 112»] comprising:

the application server receiving, from a client device, a request to direct an application [Figure 1 | Figure 4 | Figure 5A];

the application server, instructing the client device to provide profile data to an identification service operating on a third network device, the identification service having access to one or more profiles for identifying and accessing one or more data services, the profile data identifying a particular profile [Figure 1 | Figure 4 «items 106, 410, 108» | column 5 «lines 44-54» | column 10 «lines 45-55];

the identification service providing the data service with the particular profile identified by the profile data, the profile containing data for identifying and accessing the data service [Figure 4 | column 10 «lines 45-55»]; and

the data service using the profile to generate temporary credentials for accessing the data service [column 6 «lines 48-54» | column 10 «lines 55-63» where : the HTTP server generates a cookie for the user to access the protected resources, the HTTP and resources part of the access server data service].

Win does not expressly disclose that the application server obtaining the temporary credentials and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client.

23> In a related field of invention, Brown is directed towards a system for enabling a user to access protected resources. Brown further discloses a system that enables a proxy device to access protected resources using the credentials and rights of a user device Brown discloses an proxy server obtaining temporary credentials that were generated for a client, and provides a data service with the temporary credentials to access and interact with the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the temporary credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple locations[0026, 0027]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

24> As to claims 15-18, as they do not teach or further define over the claimed limitations. they are rejected for the same reasons set forth for claims 7-10, supra.

25> As to claim 19, as it does not teach or further define over the claimed limitations, it is rejected for the same reasons set forth for claim 11.

26> As to claims 21-25, as they are mediums that execute the steps of the method of claims 1-5, respectively, they do not teach or further define over the claimed limitations. Therefore claims 21-25 are rejected for the same reasons set forth for claims 1-5, supra.

27> As to claims 26-29, as they do not teach or further define over the steps of the method of claims 1-5, they are rejected for at least the reasons set forth for claims 1-5.

28> As to claim 30, Win discloses the medium having instructions for generating an interface includes generating a framed web page having a first frame and a second frame, the method further comprising providing, for the first frame, content for directing an application, and providing, for the second frame, content for selecting one or more electronic files managed by the data service identified by the specified profile [column 5 «lines 44-46» | column 6 «lines 10-16» | column 9 «lines 20-30» | column 11 «lines 33-64» | column 12 «lines 3-8 and 65-66» where : Win's roles are analogous to user profiles. And Win discloses web pages with functionality for directing an application and selecting one or more electronic files but does not explicitly disclose that the two functionalities are split amongst two frames within a page. Win does disclose that the user options are presented in a personalized HTML menu and that the browser should be compatible with frames. Further, frames are ubiquitous in the art and based on Win's suggestions, would be expected in Win's HTML pages. The claimed use of a first frame and second frame is merely matter of design choice and does not represent any patentable distinction over the prior art references].

29› As to claim 32, Win discloses a computable readable medium having instructions for:

from a third network device, generating an interface having user accessible controls for creating a profile for accessing a data service, operating on a second network device [Figure 1 | column 10 «lines 41-51» | column 11 «lines 21-32» | column 13 «line 40» to column 17 «line 38» : Win's registry server and protected server (protected resource)];

from the third network device, creating a profile according to selections made through the interface the profile containing data for identifying and accessing the data service [column 12 «lines 55-60» | column 13 «line 40» to column 17 «line 38»];

from the third network device, providing a client device with profile data identifying a created profile [column 10 «lines 41-45»];

upon receiving profile data, retrieving a profile identified by the profile data received [column 10 «lines 47-49»]; and

generating temporary credentials for accessing the data service identified by the retrieved profile [column 10 «lines 51-63»].

Win does not expressly disclose that the application server obtaining the temporary credentials and providing the data service with the temporary credentials to access the data service on behalf of the client.

30› In a related field of invention, Brown is directed towards a system for enabling a user to access protected resources. Brown further discloses a system that enables a proxy device to access protected resources using the credentials and rights of a user device Brown discloses an proxy server obtaining temporary credentials that were generated for a client, and provides a

data service with the temporary credentials to access the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the temporary credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple locations[0026, 0027]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

31> As to claims 33-36, as they are claims to a medium that execute the steps of the method of claims 2-5 respectively, they do not teach or further define over the claimed limitations. Therefore claims 33-36 are rejected for the same reasons set forth for claims 2-5.

32> As to claim 37, Win discloses instructions for providing a client device with profile data comprise instructions for generating a cookie containing data identifying the created profile and instructing a web browser operating on the client to save the cookie [Figure 5C]

33> As to claim 38, as it does not teach or further define over the previously claimed limitations (see for example, claims 1, 6, and 32), claim 38 is rejected for at least the same reasons.

34> As to claims 39-41, as they are claims to mediums that execute the steps of the method of claims 7, 8 and 10, they do not teach or further define over the claimed limitations. Therefore claims 39-41 are rejected for the same reasons set forth for claims 7, 8 and 10.

35> As to claim 42, as it is a claim to a medium that executes the steps of the method of claim 11, it does not teach or further define over the claimed limitations. Therefore, claim 42 is rejected for the same reasons set forth for claim 11.

36> As to claim 44, Win discloses a system for providing a first network resource operating on a first network device with access to a second network resource operating on a second network device, comprising:

an identification service operating on a third network device [Figure 6] in network communication with a credential module, the credential module operating on the second network device and operable to use a profile acquired by the identification service to generate temporary credentials for accessing the second network resource [Figure 2 | column 10 «lines 41-49»], the identification service being operable to receive profile data from a client device, to acquire a profile identified by the profile data [column 10 «lines 41-45»].

Win does not expressly disclose the credential module and identification service, together being operable to provide the first network resource with the temporary credentials enabling the first network resource to provide the second network resource with the temporary credentials to access the second network resource on behalf of the client device.

37> In a related field of invention, Brown is directed towards a system for enabling a user to access protected resources. Brown further discloses a system that enables a proxy device to access protected resources using the credentials and rights of a user device Brown discloses an proxy server receiving the temporary credentials that were generated for a client, and provides a data service with the temporary credentials to access the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the temporary credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple locations[0026, 0027]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

38> As to claims 45-48, as they are mediums that execute the steps of the method of claims 2-5, respectively, they do not teach or further define over the claimed limitations. Therefore claims 45-48 are rejected for the same reasons set forth for claims 2-5, supra.

39> As to claim 49, Win discloses a system for accessing a data service operating on a second network device comprising:

an identification service, operating on a third network device, operable to receive profile data from a client device identifying a particular profile and to provide that profile, the profile to contain electronic data used to identify the data service [Figure 6 | column 9 «lines 33-60» | column 10 «lines 41-63»];

a credential module, operating on a second network device, operable to obtain the profile from the identification service, generate temporary credentials, and map those credentials to the data service identified by the profile [Figure 2 | column 9 «lines 30-40» | column 10 «lines 49-63»];

an application server, operating on a first network device, operable to serve an interface containing instructions to send profile data to the identification service [Figure 1].

Win does not explicitly disclose that the application server obtains the temporary credentials, and provides the data service with the temporary credentials to access the data service on behalf of the client.

40› Brown is directed towards a system for enabling a user to access protected resources. Brown further discloses a system that enables a proxy device to access protected resources using the credentials and rights of a user device Brown discloses an proxy server receiving the temporary credentials that were generated for a client, and provides a data service with the temporary credentials to access the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the temporary credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple

locations[0026, 0027]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

41> As to claim 50, Win discloses the system wherein the credential module is further operable to invalidate the temporary credentials following a termination event [column 11 «lines 6-9»].

42> As to claim 51, Win discloses:

an application content provider in communication with the application server and operable to generate content for directing an application [Figure 4 «item 412» | column 9 «lines 28-29»]; and

a data content provider in communication with the application server and operable to generate content for selecting electronic files managed by the accessed data service [Figure 4 «item 208» | column 3 «lines 36-40»].

43> As to claim 54, Win discloses a system for accessing a data service operating on a second network device, the system comprising:

an identification service operating on a third network device and operable to generate a profile interface having user accessible controls for creating a profile containing electronic data used to identify the data service, to create a profile using selections made through the profile interface, to issue instructions to store profile data used to access the created profile, to receive from a client device, profile data identifying a particular profile, and to provide that profile [Figure 6 | column 7 «lines 45-57» | column 9 «lines 20-60» | column 10 «lines 41-55»];

a credential module operable to obtain the profile from the identification service, generate temporary credentials, and map those credentials to the data service identified by the profile [Figure 4 | column 9 «lines 30-40» | column 10 «lines 49-63»];

an application server operating on a first network device and operable to serve an interface containing instructions to send profile data to the identification service [Figure 1].

Win does not explicitly disclose that the application server obtains the temporary credentials, and provides the data service with the temporary credentials to access the data service on behalf of the client.

44> Brown is directed towards a system for enabling a user to access protected resources. Brown further discloses a system that enables a proxy device to access protected resources using the credentials and rights of a user device Brown discloses an proxy server receiving the temporary credentials that were generated for a client, and provides a data service with the temporary credentials to access the data service on behalf of the client [0019, 0020, 0022]. According to Brown, it is advantageous to provide a proxy server that obtains the temporary

credentials for a user, and access the requested services on behalf of a user because such an implementation increases the level of security and enabling user access from multiple locations[0026, 0027]. Therefore, it would have been obvious to one of ordinary skill in the art to modify Win's resource access system to include the proxy server functionality provided by Brown's teachings. The combination of Win and Brown would thus provide a system where a proxy obtains credentials of a user and accesses a data service on behalf of the user when the user makes a request for resources. One would have been motivated to provide such an implementation for the advantages discussed.

45> As to claims 55 and 56, as they not teach or further define over the limitations of claims 50 and 51 respectively, they are rejected for the same reasons set forth for claims 50 and 51.

46> As to claim 58, Win discloses the system of claim 54 further comprising a browser operable to request and display the profile and application interfaces [Figure 4].

47> As to claim 59, as it is a claim to a system that contains the functionality of the medium of claim 38, it does not teach or further define over the claimed limitations. Therefore, claim 59 is rejected for the same reasons set forth for claim 38, supra.

48› Claims 13, 20, 31, 43, 52, 53, and 57 are rejected under 35 U.S.C § 103(a) as being unpatentable over Win and, in further view of Curtin, "A Failure to Communicate: When a Privacy Seal doesn't help" ["Curtin"].

49› Curtin was cited by Examiner in previous Office Action, 4.15.2005.

50› As to claim 13, Win discloses a request including a cookie identifying a particular profile [column 10 «lines 51-54»] but does not disclose including instructions to request a web bug from the identification service, and wherein the act of sending the profile data includes requesting the web bug.

51› Curtin discloses including instructions to request a web bug from the identification service, and wherein the act of sending the profile data includes requesting the web bug [see 1.4 "Web Bugs" and "B. TheCounter.com Tracking Code" page 7]. Curtin discloses the use of the web bug to allow for web sites to track and monitor the actions of users in an almost invisible manner. Therefore, it would have been obvious to one of ordinary skill in the art to incorporate Curtin's web bug functionality into Win's resource accessing system to allow administrators access to user activity. Such a functionality would enable administrators the ability profile users and keep track of their use of web servers [see Curtin, 2.2.2 Profiling Capability and 1.4 Web Bugs].

52> As to claims 20 and 31, as they do not teach or further define over the claimed limitations, they are rejected for the same reasons set forth for claim 13.

53> As to claim 43, as it is a claim to a medium that executes the steps of the method of claim 13, it does not teach or further define over the claimed limitations. Therefore, claim 43 is rejected for the same reasons set forth for claim 13.

54> As to claims 52, 53 and 57, as it is does not teach or further define over the combined limitations of claims 11 and 13, claims 52, 53 and 57 are also rejected for the same (combined) reasons set forth for claims 11 and 13, supra.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dohm Chankong whose telephone number is 571.272.3942. The examiner can normally be reached on Monday-Thursday [7:00 AM to 5:00 PM].

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571.272.3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DC

BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER